REMARKS

The Examiner has rejected Claims 1, 2, 4-9, 19-27 and 37-42 under 35 U.S.C. 103(a) as being unpatentable over CNN (http://www-cgi.cnn.com/TECH/computing/9907/ 21/badrap.idg/). Applicant respectfully disagrees with such rejection for the reasons stated below.

The Examiner has argued that applicant's arguments were not persuasive. As set forth below, such rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of dependent Claim 4 et al. into independent Claims 1, 8, 9, 19, 26 and 27 (as originally incorporated, at least in part, into independent Claim 37).

With respect to each of the independent claims, the Examiner has responded to applicant's arguments by stating that "CNN teaches sending the information to the researcher, hence suggesting sending encrypted information to a plurality of remote locations" and "CNN teaches quarantining, hence suggesting blocking of the malicious code for a period of time based on the information."

Again, applicant respectfully asserts that CNN does not teach applicant's claimed "sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network; and blocking instances of the malicious code at the remote locations for a predetermined amount of time based on the information" (see this or similar, but not identical, language in each of the independent claims).

First, CNN does not teach "encrypted information relating to...malicious code," as applicant claims. The Examiner has relied on CNN's disclosure of "Trojans [that] are delivered as attachments in e-mail...[that can be] destroy[ed] or quarantine[d]...in order to send them to [a] researcher" (see paragraph quoting Symantec) to meet applicant's claimed "sending encrypted information relating to the malicious code." Simply nowhere in CNN's disclosure is there any mention of "encrypted information," and

especially not of "encrypted information relating to malicious code." The destroyed or quarantined Trojan itself is what is sent to the researcher, and not any encrypted information relating to the Trojan.

Second, CNN does not teach "sending the encrypted information...to a plurality of remote locations utilizing the network" as claimed by applicant. Again, the Examiner has relied on CNN's disclosure of sending the destroyed or quarantined Trojan to a researcher to meet applicant's claim language. Applicant respectfully asserts that CNN only discloses sending the destroyed or quarantined Trojan to a single researcher. In addition, CNN does not teach that such researcher is a remote location. Thus, CNN clearly cannot teach or even suggest "sending the encrypted information...to a plurality of remote locations utilizing the network" (emphasis added).

Third, CNN does not teach "blocking instances of the malicious code at the remote locations for a predetermined amount of time based on the information," as claimed by applicant. Yet again, the Examiner has relied on CNN's disclosure of quarantining a Trojan to meet applicant's claim language. However, CNN does not teach that the researcher is the device that quarantines the Trojan, but instead that the researcher merely receives the quarantined Trojan. Thus, the researcher as disclosed in CNN is simply utilized for receiving such information, and not for blocking it, in the context claimed by applicant.

Further, CNN does not even mention any sort of blocking "for a predetermined amount of time based on the information," as claimed by applicant. In CNN, the Trojan is simply destroyed, in which case the destruction is permanent, or quarantined and sent to the researcher, in which case there is no further disclosure in CNN of whether the Trojan is quarantined only for a predetermined period of time based on the information.

With respect to applicant's claimed technique "wherein the information relating to the malicious code includes an identification of the source of the malicious code, wherein communications originating at the identified source are denied access to the remote

locations for the predetermined amount of time" (see each of the independent claims), applicant respectfully asserts that identification of the source of the malicious code would not be necessary for destroying and quarantining a Trojan along with sending the destroyed or quarantined Trojan to a researcher, as disclosed in CNN, since all that is needed for such operations is the Trojan itself. The identification of the source of the Trojan is simply unnecessary in such operation, and thus is not required for Symantec's software to run. To this end, the Examiner's argument is deficient.

Furthermore, applicant claims denying access to remote locations by the malicious code to remote locations based on the identified source for a predetermined amount of time. This is vastly different from CNN's suggestion of simply destroying a Trojan at the local location it was discovered, or quarantining such Trojan. Clearly, it is only the Trojan described in CNN that is being denied access due to its destruction or quarantined state, and not all communications originating at the identified source, in the manner claimed by applicant.

Also with respect to each of the independent claims, the Examiner states that encrypting information is well known in the art for the motivation of hiding information from a hacker who appears to be using a malicious code to seize control of a system, and acknowledges that CNN does not teach encrypting information, as claimed by applicant. Applicant respectfully disagrees with this assertion.

In invoking such Official Notice, the Examiner has failed to recognize the full weight of applicant's claims. Specifically, applicant teaches and claims encrypting information relating to malicious code, and not simply encrypting *any* information in order to hide it from a hacker. Applicant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

> "If the applicant traverses such an [Official Notice] assertion the examiner should cite a

> reference in support of his or her position." See MPEP 2144.03.

In addition, the CNN reference clearly fails to teach "encrypting information relating to the malicious code at the local location" (emphasis added). CNN does not teach encrypting information in any manner, let alone information relating to malicious code that was identified at the local location and also encrypting such information also at the local location.

Further, the Examiner has relied on the following excerpt from CNN to make a prior art showing of applicant's claimed "sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network; and blocking instances of the malicious code at the remote locations for a predetermined amount of time based on the information."

> "It's just another Trojan horse for us," says Darren Kessner, Symantec's senior virus researcher. "Most Trojans are delivered as attachments in e-mail, and with our Norton Anti-Virus product, you now have an option to destroy or quarantine them in order to send them to our researcher."

Again, applicant respectfully disagrees with this assertion. CNN simply states that when a Trojan is found at a local location, a user has the option to either destroy that Trojan at the local location or quarantine the Trojan in order to send it to a researcher. Thus, CNN does not even suggest sending encrypted information relating to the malicious code to a plurality of remote locations, nor does it suggest blocking instances of the malicious code at those remote locations for a predetermined amount of time based on the information. CNN thus fails to give any indication that encrypted information relating to identified malicious code is sent to multiple remote locations such that those locations can block instances of the malicious code for predetermined amounts of time.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or

in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art reference fails to teach or suggest all the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claim 4 into independent claims 1, 8, 9, 19, 26 and 27 (as originally incorporated, at least in part, into independent Claim 37). With respect to the subject matter of dependent Claim 4, the Examiner has simply dismissed the same under official notice and has stated that such particular features are well known in the art for the purpose of handling information across computers.

However, in making such a statement, it seems the Examiner has not considered the full weight of applicant's claimed "registering at least one of a name and checksum of a file containing the malicious code as a known threat." Applicant respectfully asserts that registering a name and/or checksum of file as a known threat, in the specific manner claimed by applicant, is not well known for simply handling information across computers, as suggested by the Examiner. Applicant claims registering, as a known threat, a name and/or checksum "of a file containing the malicious code." Thus, the file may be identified since it is registered by name and/or checksum as being a known threat.

Applicant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Again, note the excerpt from MPEP below:

"If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

CNN is further deficient with respect to applicant's dependent claims. For example, with respect to dependent Claims 5-8, and 11-36, the Examiner has simply dismissed the same under Official Notice. In response, applicant again points out the remarks above. Applicant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Again, note the excerpt from MPEP below:

"If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

In addition, the Examiner has completely failed to even address the dependent claims added in the last amendment (Claims 38-42). Thus, applicant respectfully requests consideration of such claims in view of the arguments given above.

Yet again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art reference fails to teach or suggest all the claim limitations. A notice of allowance or a specific prior art showing of each of the foregoing limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claim 43 below, which is added for full consideration.

"wherein a simple mail transfer protocol (SMTP) is utilized for collecting the information that is associated with spam attempts, spam-relay attempts, denial of service (DoS) attacks, and malicious attachment forwarding; a net news transfer protocol (NNTP) is utilized for collecting the information that is associated with

DoS attacks, malicious attachment forwarding, and cross-posting; a file transfer protocol (FTP) is utilized for collecting the information that is associated with DoS attacks, and repeated unsuccessful logins; a hypertext transfer protocol (HTTP) is utilized for collecting the information that is associated with malicious content, DoS attacks, and known hacking attempts; and a firewall protocol is utilized for collecting the information that is associated with intrusion detection, and port scanning attempts" (see Claim 43).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P025/01.156.01).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100